Reg. No.												

Question Paper Code	11474

B.E./B.Tech. - DEGREE EXAMINATIONS, NOV/DEC 2022

Seventh Semester

Computer Science and Engineering

(Common to Information Technology)

CS8792 - Cryptography and Network Security

(Regulations 2017)

Duration: 3 Hours Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

Marks, K-Level, CO

1. Examine the cipher text for the following using one time pad cipher. *2,K2,CO1*
   Plain Text: KRCT Keyword: EXAM
2. Define steganography. *2,K1,CO1*
3. Find GCD (1970, 1066) using Euclid's algorithm. *2,K3,CO2*
4. Compare DES and AES with example. *2,K2,CO2*
5. State Euler's Theorem. *2,K1,CO3*
6. Perform encryption for the plain text M=88 using the RSA algorithm p=17, q=11 and the public component e=7. *2,K3,CO3*
7. Compare MAC and Hash function. *2,K2,CO4*
8. Point out any 2 applications of X.509 Certificates. *2,K2,CO4*
9. Classify the services provided by PGP. *2,K3,CO5*
10. Compare the three classes of Intruders. *2,K2,CO5*

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11. a) Build the network security model and its important parameters with a neat block diagram. *13,K2,CO1*

OR

b) Compare the following cipher techniques to decrypt the word "PAY MORE MONEY" and Key "ENGINEERING" (i) Hill cipher (ii) Railfence cipher With depth 2 (iii) Vignere cipher. *13,K2,CO1*

12. a) Examine the properties that are to be satisfied by Groups, Rings and Fields and list the features which are essential for the exact realization of the network. *13,K2,CO2*

OR

K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyze; K5 – Evaluate; K6 – Create

b) Interpret the each of the following elements of DES, indicate the comparable element in AES if available. (i) XOR of subkey material with the input to the function. (ii) F function (iii)Permutation p (iv) Swapping of halves of the block. *13,K3,CO2*

13. a) Compare and Contrast Fermat's and Euler's theorem with an example. *13,K4,CO3*

OR

b) Construct ElGamal Cryptosystem. Using ElGamal Scheme, let α = 5, p =11, XA= 2. Find the value of YA. α = 5, p =11, XA= 2. *13, K3,CO3*

14. a) With a neat diagram, analyze and explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than 2128 bits and produces as output a 512-bit message digest. *13, K3,CO4*

OR

b) Explain with the help of an example and evaluate how a user's certificate is obtained from another certification authority in x509 scheme. *13, K3,CO4*

15. a) How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components. *13, K3,CO5*

OR

b) Evaluate the technical details of firewall and describe any three types of firewall with neat diagram. *13, K3,CO3*

PART - C (1 × 15 = 15 Marks)

16. a) Experiment the Encryption and Decryption process using Hill Cipher for the following Message: PEN and Key: ACTIVATED. *15,K2,CO1*

OR

b) Users Alice and Bob use the Diffie Hellman key exchange technique with a common prime q=83 and a primitive root alpha=5. Evaluate (i) If Alice has private key XA =6 what is Alice's public key YA? (ii) If Bob has private key XB =10 what is Bob's public key YB? (iii) What is the shared secret key? *15,K3,CO3*